Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network

Hemang Kothari [1] and Manish Chaturvedi [2]

1 Department of Computer Science and Engineering, Nirma University.
2 Department of Computer Science and Engineering, Nirma University.

E-Mails: 09mce008@nirmauni.ac.in; manish.chaturvedi@nirmauni.ac.in
DOI http://dx.doi.org/10.7125/APAN.32.11

Abstract: A multi hop mobile ad hoc network is a peer to peer network of wireless nodes where nodes are required to perform routing activity to provide end to end connectivity among nodes. As mobile nodes are constrained by battery power and bandwidth, some nodes may behave selfishly and deny forwarding packets for other nodes, even though they expect other nodes to forward packets to keep network connected. We simulate two selfish behaviors on top of Dynamic Source Routing (DSR) protocol: the first, selfish nodes do not forward data or control packets (routing packets) for other nodes and the second, selfish nodes turn off their network interface card when they have nothing to communicate. We compare the energy saving to the selfish nodes for both the misbehaviors and show that the second selfish behavior saves more energy. This is important result because most of the cooperation enforcement mechanisms in literature, except PCOM [2], address the first selfish behavior. Also, the second selfish behavior can be easily done by layman users without any protocol level changes. Secondly, with our simulation study we find that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consume significant fraction of node energy and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes.

Keywords: Mobile Ad Hoc Network, DSR, Selfish Behavior, Energy Consumption.

1. Introduction

A Mobile Ad hoc Network is a collection of wireless nodes communicating with each other in the absence of any infrastructure. Due to this infrastructure less feature, all networking functions must be performed by the nodes themselves. Packets sent between distant nodes are expected to be relayed by intermediate nodes, which act as routers and provide the forwarding service. As mention in [1] mobile nodes are typically constrained by power and computing resources, a selfish node may not be willing to use its computing and energy resources to forward packets that are not directly beneficial to it, even though it expects others to forward packets on its behalf.

In this work, we analyze the effect of selfish behavior on energy consumption in MANET. We studied various selfish behaviors in literature (Section 2: Related Work) and identified the following two representative selfish behaviors for simulation and analysis: 1) forwarding node selfish behavior: selfish nodes do not forward data or control packets (routing packets) for other nodes and 2) network card on/off selfish behavior: selfish nodes turn off their network interface card when they have nothing to communicate. We compare the energy saving to the selfish nodes for both the misbehaviors and show that the second selfish behavior saves more energy. We consider this as an important finding because as per our knowledge almost all the cooperation enforcement mechanisms except PCOM [2] address the first selfish behavior. Please refer to [1, 4, 5, 6, 14, 15] for cooperation enforcement mechanisms addressing forwarding node selfish behavior.

Secondly, we find that in dense mobile topology ad hoc networks selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes. We find that in mobile topology network scenario route caching mechanism of DSR is not effective and every link break results in route request flooding in the network. As in the dense network there are excessive number of nodes participating in route discovery, selfish behavior by certain number of nodes prunes some route discovery paths which in turn reduces the overall energy consumption of selfish nodes and other nodes along the pruned path and still keeps network connected.

This paper is organized as follows: section 2 discusses related work; Section 3 is about simulation setup; section 4 presents simulation analysis; and section 5 presents our major conclusions and future work.

2. Related Work

The limitation in energy resources along with the multi-hop nature of Mobile Ad hoc Networks (MANETs) causes a new vulnerability that does not exist in traditional networks. To preserve its own battery, a node may behave selfishly. We identified following selfish behavior from literature. In Forwarding Node Selfish Behavior [6], selfish nodes do not participate correctly in routing function by not advertising available routes or by not forwarding route request packets. Consequently, such selfish nodes will not appear on packet forwarding path. In MAC Selfish Behavior [7], a selfish host can deliberately misuse the MAC (Medium Access Control) protocol to gain more network resources than well behaved hosts. For example, IEEE

802.11 requires hosts competing for the channel to wait for backoff interval before any transmissions. A selfish host may choose to wait for a smaller backoff interval, thereby increasing its chance of accessing the channel and hence reducing the throughput share received by well-behaved stations. In Packet Dropper misbehavir [8], a selfish node drops all the data packets which come to them for forwarding. This is the most studied misbehavior in literature and most of the existing solutions to deal with this misbehavior rely on the watchdog mechanism [1]. In Partial Dropping misbehavir [9], selfish node circumvents the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold. In False Misbehavior Accusations misbehavir [9], a node may falsely report other innocent nodes in its neighborhood as misbehaving to avoid getting packets to forward. In Insufficient Transmission Power selfish behavior, a Selfish node controls its transmission power to circumvent the watchdog at the neighbor nodes. If the toppoly is A-B-C and if A is closer to B than C, then B could attempt to save its energy by adjusting its transmission power and makes it strong enough to be overheard by the predecessor node (A) but less than the required power to reach the true recipient (C). Selfish nodes can also take advantage of Imperfect Monitoring mechanisms [10]. When the miss detect ratio is high, a selfish node can always drop other nodes' packets but still claim that it has forwarded. In Set TTL Field to Zero selfish behavior [11], a selfish node may drop routing packets or forward with a time-to-live (TTL) of 0 so that no paths passing through them can be established. A selfish node could thereby avoid forwarding many subsequent data packets. Another selfish behavior is to make paths that include selfish node seem longer than they really are, perhaps by artificially increasing hop counts [11] so the source nodees are more likely to choose other routes those appear to be shorter. A selfish user may disobey the rules to access the wireless channel in order to obtain a higher throughput than the other nodes [12]. A selfish user can also change the congestion avoidance parameters of TCP in order to obtain unfair advantage over the rest of the nodes in the network. Also, a selfish user can manipulate rules of the MAC layer. In 802.11, the selfish node can manipulate the size of the Network Allocation Vector (NAV) and assign large idle time periods to its neighbors, it can decrease the size of Interframe Spaces (both SIFS and DIFS), it can select small backoff values, it can un-authenticated neighboring nodes etc. In Emulate Link Breakage selfish behavior [13], when source node (A) want to transmit packet to next node (B) on certain route R, if B is selfish , it can simply keep silent to let A believe that B is out of A's transmission range. The laymen uses without skills to falsify program codes or data maliciously can follow Network Card On/Off selfish behavior [2]. This behavior involves refusing to forward any control or data packets for others by turning off the power of network card or by turning off the communication function when they do not need to communicate.

We simulated two selfish behaviors from literature study 1) forwarding node selfish behavior: selfish nodes do not forward data or control packets (routing packets) for other nodes and 2) network card on/off selfish behavior: selfish nodes turn off their network interface card when they have nothing to communicate. We simulate forwarding node selfish behavior because it targets forwarding functionality of DSR protocol and most of the research work has been done on this selfish behavior. So we need to evaluate whether this behavior saves more energy compare to other selfish behavior specified in literature. We simulate network card on/off behavior [2] because it can easily deployed by laymen user.

3. Simulation

Simulations have been carried out in order to analyze the effect of selfish behavior on network card power function and packet forwarding function of DSR [3] protocol. We focused our attention on the evaluation of network performance in terms of routing overhead, throughput and energy consumption of a mobile ad hoc network where a defined number of nodes were misbehaving.

3.1 Simulation Setup

We conducted exhaustive simulations in the simulation tool NS-2.34[20, 21]. The simulation parameters are listed in Table 1. We used Random Way Point model [18] because we were not targeting particular application. In each traffic pattern, 50 sessions are constantly maintained to keep every node involved in networking. The results are averaged of 10 simulation rounds conducted with various random seeds. We set maximum number of packet as 10000 for forwarding node misbehavior which is large enough to continue session till end of the simulation time. We also set maximum number of packet as 300 for network card on/off misbehavior which is large enough to see the effect of this selfish behavior. Physical layer parameters are taken according to wavelan card specification [16, 17].

Table 1. Simulation Parameter.

General Parameter		**Energy Model Parameter**	
Number of Nodes	50	Transmit Power	1.65 W
Topology	Static & Mobile	Receiving Power	1.40 W
Simulation Time	1000	Sleep Mode	0.045 W
MAC Layer	802.11	Idle Mode	0.843 W
Range	200 meters	Initial Energy	1500 J
Simulation Area	1000 x 1000 $meter^2$		
Traffic Model Parameter			
Traffic Model	Constant Bit Rate	Traffic Model	Poisson
Packet Size	512 Bytes	Interval	1 Sec
Interval	1 Sec	Rate	1 Mb

4. Observations

4.1. Forwarding Node Selfish Behavior

Selfish node does not perform packet forwarding function of DSR protocol. Node with this kind of selfish behavior also does not participate in route discovery phase of DSR protocol.

4.1.1. Static Topology with Constant Bit Rate Traffic

In static topology, routes are established at the beginning of session and remain valid throughout the session. So route overhead is low compare to dynamic topology and do not consume more energy. From *Figure 1* we can say that as number of selfish node increase in network, good node need to do more work to compensate the selfish node work. So good node need to spend more energy to complete the work. Simulation result show that selfish nodes save more energy as number of selfish node increase in network.

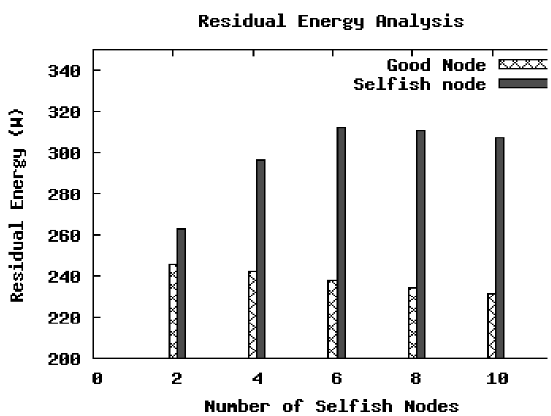


Figure 1. Residual Energy Vs Number of Selfish Nodes for static topology

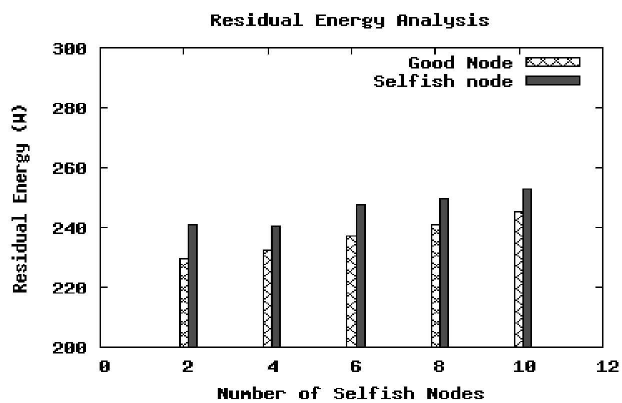


Figure 2. Residual Energy Vs Number of Selfish Nodes for dynamic topology

4.1.2 Dynamic Topology with Constant Bit Rate Traffic

Figure 2 shows the simulating result of dynamic topology network scenario. In this scenario as well, good nodes consume more energy than selfish nodes. However the energy saving increases for good nodes as well as selfish nodes as number of selfish nodes increase in network. This is counter intuitive and we identified following reason for it:

In mobile topology network scenario, link breakages are frequent and routing caching mechanism of DSR is not effective. So routing overhead is a major component in energy consumption. When node density is high and all the nodes participate in flooding based route discovery, nodes consume more energy. When some nodes behave selfishly, they prune all route requests coming to them. This behavior saves energy for the selfish nodes and all the other nodes following the node on path towards destination. This has the effect of reducing the node density of network. So selfish nodes reduce number of control packet in network hence reduce energy consumption of good nodes as well as selfish nodes.

Figure 3 shows that as number of selfish nodes increases in dynamic topology dense network, the routing overhead decreases. Routing overhead is monitored in terms of number of routing control packets in the network. Due to drastic decrease in routing overhead, overall network become efficient and good nodes as well as selfish nodes saves energy.

Figure 4 shows the throughput of network with varying number of selfish nodes. Throughput is measured as ratio of total number of packets successfully delivered to destination nodes and total number of packets generated by source nodes. As number of selfish nodes increases up to certain level, the network throughput increases due to reduction in number of collisions. We observe the decrease in throughput after the threshold point (more than twenty selfish nodes in network). This is due to the fact that as more and more nodes behave selfishly, network becomes partitioned and nodes face difficulty in establishing end to end path from source to destination.

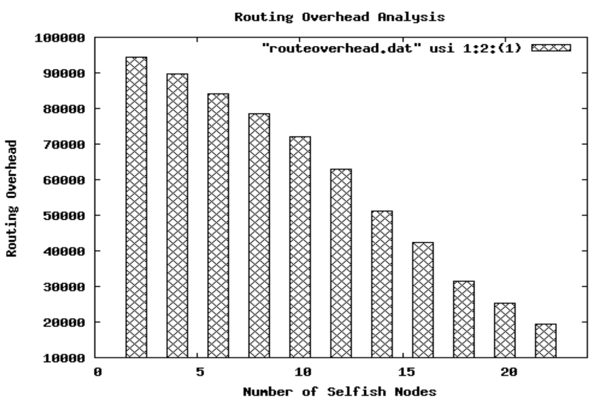


Figure 3. Route overhead Vs Num. of Selfish Nodes

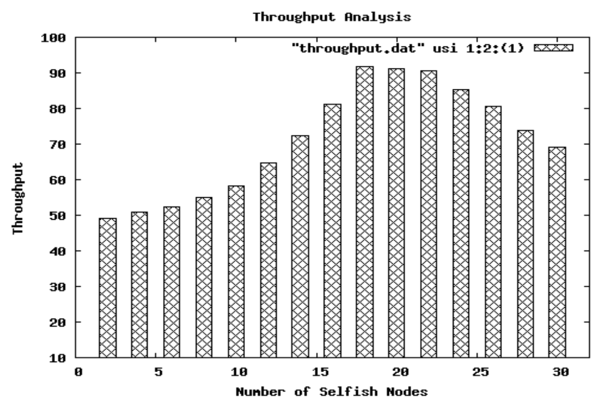


Figure 4. Throughput Vs Num. of Selfish Nodes

4.1.3 Dynamic Topology with Poisson Traffic

As we obtained counter intuitive results for energy consumption of nodes in dynamic topology mobile ad hoc network for CBR traffic (both good nodes and selfish nodes save energy as number of selfish nodes increases), we wanted to validate our simulation results for Poisson traffic as well. Figure 5 shows the simulation results of dynamic topology network scenario with Poisson traffic. In this scenario as well, good nodes consume more energy than selfish nodes. However the energy saving increases for good nodes as well as selfish nodes as number of selfish nodes increase in network. This is the similar result as we obtained for CBR traffic: In mobile topology network scenario, routing overhead is a major component in energy consumption and selfish behavior by certain number of nodes reduces the routing overhead significantly in the network which in turn results in energy saving for both, the good nodes as well as the selfish nodes.

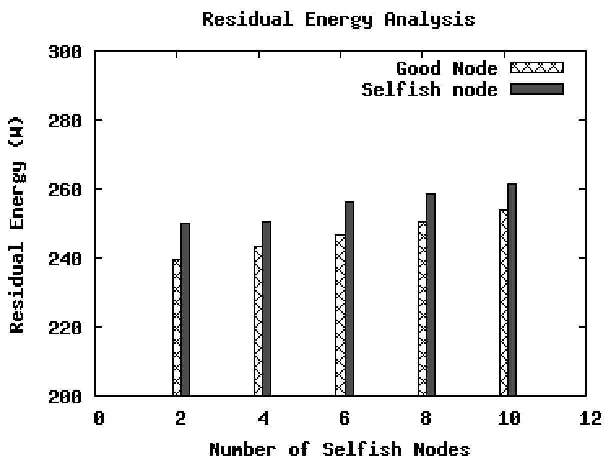


Figure 5. Residual Energy Vs Number of Selfish Nodes

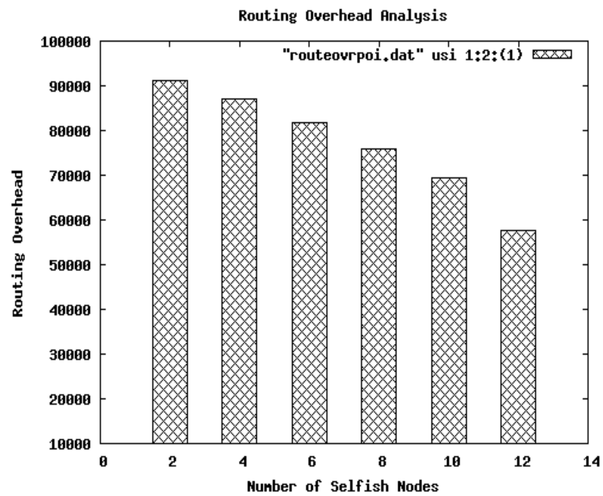


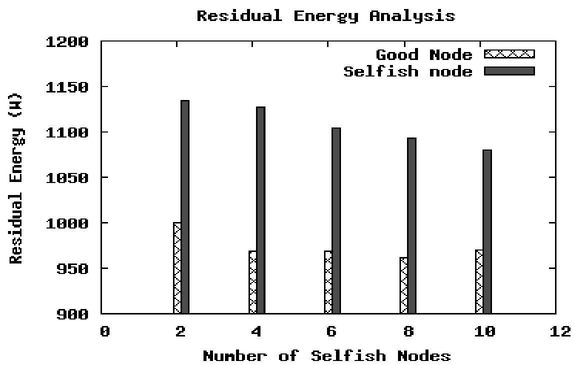
Figure 6. Route overhead Vs Num. of Selfish Nodes

Figure 6 shows that as number of selfish nodes increases in dynamic topology dense network, the routing overhead decreases. Routing overhead is monitored in terms of number of routing control packets in the network. Due to drastic decrease in routing overhead, overall network become efficient and good nodes as well as selfish nodes saves energy.

4.2. Wireless Network Card On/Off Selfish behavior

4.2.1. Static Topology with CBR Traffic

Figure 7 shows effect of number of selfish nodes on energy consumption of good nodes and selfish nodes for static topology network scenario. Here also selfish nodes save more energy than well behaving nodes but energy saving for selfish nodes is much more with this selfish behavior when compared to that with forwarding node selfish behavior.



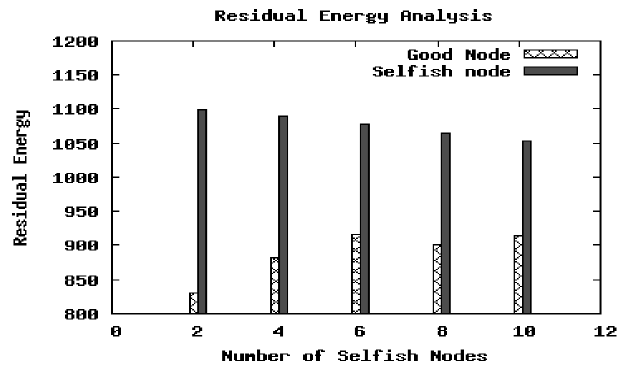


Figure 7. Residual Energy Vs Num. of Selfish Node For Static Topology

Figure 8. Residual Energy Vs Num. of Selfish Node For Dynamic Topology

4.2.2. Dynamic Topology with CBR Traffic

Figure 8 shows effect of number of selfish nodes on energy consumption of good nodes and selfish nodes for dynamic topology network scenario. Here also selfish nodes save more energy than good nodes. With this selfish behavior as well, as number of selfish nodes increases in network, good nodes also save energy. The main reason for this is reduction in routing overhead as more and more nodes turn off their network card.

4.3 Comparison of Selfish Behaviors

Figure 9 shows the comparison between energy consumption of two selfish behaviors that we have simulated, namely, forwarding node misbehavior and network card on/off selfish behavior. Simulating result shows that Network Card On/Off Selfish Behavior saves much more energy compare to Forwarding Packet Selfish Behavior for selfish nodes.

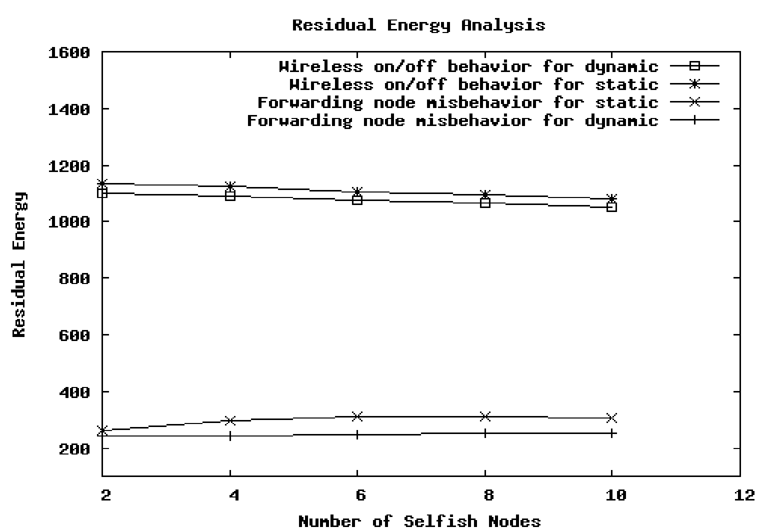


Figure 9. Comparison of Selfish Behaviors

We consider this as an important finding because as per our knowledge almost all the cooperation enforcement mechanisms except PCOM [2] address the first selfish behavior [1, 4, 5, 6, 14, 15]. Figure 9 shows residual energy of selfish nodes only.

5. Conclusion

In this paper, we simulate two representative selfish behaviors namely forwarding node selfish behavior and network card on/off selfish behavior on top of DSR. We compare the energy saving to the selfish nodes for both the misbehaviors and show that network card on/off selfish behavior saves more energy. This is very important observation because most of the cooperation enforcement mechanisms proposed in literature addresses the forwarding node selfish behavior.

Secondly, with our simulation study we find that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consumes significant fraction of node energy and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes.

References

1. Sergio Marti; T.J. Giuli; Kevin Lai; Mary Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Proceedings of Mobicom 2000*, Boston, USA, August 2000.
2. Toshihiro Suzuki; Motonari Kobayashi; Ashiq Khan; Masanori Morita. Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad hoc Networks. *IEICE Transactions on Communication*, Istanbul, June 2006; Volume E90.
3. David B.; Johnson David A.; Maltz Josh Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. *Ad Hoc networking 2001*; Vol 5, pp. 139-172.
4. Levente Buttyan; Jean-Pierre Hubaux. Enforcing Service Availability in Mobile Ad-Hoc WANs. *1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000)*, Boston, MA, USA, 11 August 2000.
5. Mandalas, K.; Flitzanis, D.; Marias, G.F.; Georgiadis, P. A survey of several cooperation enforcement schemes for MANETs. *Proceedings of the Fifth IEEE International Symposium* on 21-21 Dec. 2005, Athens; pp. 466 – 471.
6. Abdelaziz Babakhouya; Yacine Challal; Abdelmadjid Bouabdallah. A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks. 2008 IEEE, DOI 10.1109/NGMAST.2008.56.
7. Lei Guang; Chadi Assi. Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks. *2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communication 2006 (Wimob2006)*; pp. 116-123.

8. Tarag Fahad; Djamel Djenouri; Robert Askwith. On Detecting Packets Droppers in MANET: A Novel Low Cost Approach. *In Proceedings of Third International Symposium on Information Assurance and Security 2007(IAS'07)*; pp. 56-64.
9. Djamel Djenouri; Nadjib Badache. Two Hops ack: New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks. *Technical Report LSI-TRO704*, University of Science and Technology houari boumediene, Algeria, April 2003.
10. Wei Yu; K. J. Ray Liu. Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach. *IEEE transactions on information forensics and security*, June 2008; vol. 3, no. 2.
11. Hyun Jin Kim; Jon M. Peha. Detecting Selfish Behavior in a Cooperative Commons. In *Proceedings of IEEE DySPAN 2008*; pp. 1-12.
12. A. A. C´ardenas; S. Radosavac; J. S. Baras. Detection and prevention of MAC layer misbehavior in ad hoc networks. In *Proceedings of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks 2004*, SASN, Washington, DC, USA; pp. 17–22.
13. Wei Yu; K. J. R. Liu. Attack-resistant cooperation stimulation in autonomous ad hoc networks. *Selected Areas in Communications, IEEE Journal*, December 5, 2005; Vol. 23, No. 12, pp. 2260-2271.
14. P. Michiardi; R. Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proc. 6th IFIP Commun. and Multimedia Security Conf.*, Sept. 2002.
15. S. Bansal; M. Baker. Observation-Based Cooperation Enforcement in Ad-hoc Networks. Technical Report, Stanford University, 2003.
16. Lucent Technologies. WaveLan IEEE 802.11 PC Card User's Guide. February, 1999.
17. L. M. Feeney; M. Nilsson. Investigating the Energy Consumption of a Wireless Network Intrface in an Ad Hoc Networking Environment. *IEEE INFOCOM-2001*.
18. Jungkeun Yoon; Mingyan Liu; Brian Noble. Random Waypoint Considered Harmful. *IEEE INFOCOM-2003*.
19. Andrej KOS; Janez BASTER. Poisson Packet Generation based on Empirical Data. *Systmics, Cybernetics and Informatics 2006*; volume1, number5.
20. Network Simulator Documentation at http://www.isi.edu/nsnam/ns/
21. Mobility Trace analyzer tools at http://nile.cise.u.edu/important/software.htm